Classification Title: INFORMATION TECHNOLOGY MANAGER I	**Branch/Division/Bureau:** EXECUTIVE OPERATIONS
Working Title: Chief Information Security Officer	**Office/Unit/Section/Geographic Location:** Enterprise Planning, Risk and Compliance Office///SACRAMENTO (300)
Position Number (13 Digit): 413-109-1405 001	**Conflict of Interest Position:** YES
Employee Name:	**Effective Date:**

BASIC FUNCTION:

Under the general direction of the Enterprise Planning, Risk and Compliance Chief, the Chief Information Security Officer (CISO) has significant responsibility for providing direction and oversight related to the implementation of information security practices ensuring protection of the California Department of Insurance (CDI) assets. The incumbent oversees the Development, implementation, and maintenance of enterprise policies, standards, procedures, and guidelines to ensure the security, confidentiality, integrity, availability, and privacy of CDI's information assets. The incumbent must maintain the confidentiality of information acquired while performing job duties, demonstrate ethical behavior, and work close and cooperatively with the Information Technology Division (ITD), CDI's Privacy Officer, and other internal and external partners. The position requires the incumbent to travel up to 10% of the time.

This position is designated under the Conflict of Interest Code. The position is responsible for making or participating in the making of governmental decisions that may potentially have a material effect on personal financial interests. The appointee is required to complete Form 700 within 30 days of appointment. Failure to comply with the Conflict of Interest Code requirements may void the appointment.

ESSENTIAL FUNCTIONS*

35% Formulates, implements, and administers a comprehensive information security program to ensure compliance with policies and standards. Develops and implements strategic vision to streamline and improve policies, procedures, standards, and guidelines, which will enhance CDI's overall security position. Works collaboratively with peers in ITD, CDI's Privacy Officer, executives, and the lines of business to continuously improve the processes, procedures, standards, and guidelines, which will enhance CDI's overall security posture. Conducts maturity assessments to identify gaps and develop alternatives for investment and develops corrective actions to base on discovered vulnerabilities. In collaboration with ITD, ensures information security requirements are addressed in developing a Departmental and Department information security architecture roadmap.

25% Provides direct supervision, leadership, and policy direction to the Information Security staff responsible for risk identification, threat detection, analysis, investigation, incident response, security monitoring, security consulting, and vulnerability assessments. Organizes, prioritizes, and directs staff workload. Develops annual goals, and objectives as well as workload and performance measures. Oversees the activities of information security staff; establishes priorities for staff and vendors assigned to team efforts; establishes work standards and measurements for the team; reviews work for completeness, accuracy, schedule conflicts, and fulfillment of requirements. Performs employee evaluations, completes probation reports and annual appraisals; responsible for staff training and development; responsible for managing issues and risks, and reporting program status to management and customers. Conducts recurring "one on one" meetings with direct reports. Recruits, develops, and retains a competent professional staff that assures an adequate level of specialized technical expertise to support current and future CDI's information security needs. Coordinates and facilitates information security assessments.

25% Serves as the information security expert in CDI governance councils and organization-wide forums. Advises and consults on matters related to business continuity and the mitigation of business disruption. Participates in Enterprise Risk Management meetings as needed. Develops physical security criteria checklist. Provides expertise in industry standards. Reviews penetration tests and security control reports to determine an appropriate response. Oversees and facilitates CDI's

Information Security Awareness Training. Manage threats and incidents impacting CDI's information security posture. Reports data breaches, determines authenticity of reported security violations, reviews security incident reports, and develops a response to data breaches.

10% Provides oversight activities in the development, test, and implementation of the CDI TRP to support the requirements of the State Administrative Manual, OIS, State and federal regulations. Works with programs to identify mission-critical systems and data.

MARGINAL FUNCTIONS

5% Performs administrative duties including, but not limited to: adheres to Department policies, rules, and procedures; submits administrative requests including leave, overtime, travel, and training in a timely and appropriate manner; accurately reports time and submits time into the appropriate time accounting system by the due date.

WORK ENVIRONMENT OR PHYSICAL ABILITIES

- The incumbent may work in a shared internal office and/or in a high-rise office building.

I have read and understand the duties listed above and I can perform these duties with or without reasonable accommodation. (If you believe reasonable accommodation is necessary, discuss your concerns with the hiring supervisor. If unsure of a need for reasonable accommodation, inform the hiring supervisor, who will discuss your concerns with the Health & Safety Analyst.)

_____
Employee Signature Date

_____
Printed Name

I have discussed the duties of this position with and have provided a copy of this duty statement to the employee named above.

_____
Supervisor Signature Date

_____
Printed Name